Perancangan Algoritma *Message Authentication Code (MAC)* Dengan Pendekatan Kriptografi *Block Cipher* Berbasis 256 Bit Pada Pola Papan *Dart*

[1]Aldrien Wattimena, [2]Magdalena A. Ineke Pakereng, [3]Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email: [1)]672011156@student.uksw.edu, [2)]inekep200472@yahoo.com,
[3)]alzdanny.wowor@staff.uksw.edu

Abstract

Message Authentication Code (MAC) is one technique for securing the authentication of a message digitally. Message Authentication Code (MAC) is also used to maintain the message's integrity of change by the third parties. In this study, Message Authentication Code (MAC) algorithm is designed approaching to 256 bit cryptographic block cipher-based on dart board pattern, then the process of encrypting plaintext (message) is designed as four processes consisting of twenty rounds at each process to get the ciphertext after XOR-ed with a key that has been regenerated before being compressed to get a Message Authentication Code (MAC). The results of this study can be used as an alternative for data security algorithms using Message Authentication Code (MAC) algorithm is designed approaching to 256 bit cryptographic block cipher-based on dart board pattern.

Keywords: *Message Authentication Code, Block Cipher, Dart Board Pattern*

Abstrak

Message Authentication Code (*MAC*) adalah salah satu teknik untuk mengamankan otentikasi pesan secara digital. *Message Authentication Code* (*MAC*) juga digunakan untuk menjaga integritas pesan dari perubahan pihak ketiga. Pada penelitian ini dirancang sebuah algoritma *Message Authentication Code* (*MAC*) dengan pendekatan kriptografi *block cipher* berbasis 256 bit pada pola papan *dart*, kemudian proses enkripsi *plaintext* (pesan) dirancang sebanyak empat proses yang terdiri dari dua puluh putaran pada tiap-tiap proses untuk mendapatkan *ciphertext* setelah di-XOR dengan kunci yang sudah diregenerasi sebelum dikompresi untuk mendapatkan nilai *Message Authentication Code* (*MAC*). Hasil dari penelitian ini dapat digunakan sebagai alternatif pengamanan data menggunakan algoritma *Message Authentication Code* (*MAC*) dengan pendekatan kriptografi *block cipher* berbasis 256 bit pada pola papan *dart*.

Kata Kunci: *Message Authentication Code, Block Cipher,* Pola Papan *Dart*

[1)]Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.
[2)]Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.